In the Claims

The status of claims in the case is as follows:

1. [Currently amended] Method for operating a first node in a network including at least one second node, comprising the steps of:

establishing at said first node a coincident endpoint for an outer connection and an inner connection with respect to at least one second node, said outer connection and said inner connection being IP security connections;

responsive to receiving ~~a nested~~ an inbound nested packet from said second node on said outer connection, decapsulating said packet into a first packet and then performing source-in network address translation on said first packet; and

responsive to receiving ~~a second~~ an outbound second packet at said inner connection, performing source-in network address translation on said second packet, and then encapsulating said second packet into a nested

packet for communication on said outer connection to said second node.

2. [Canceled]

3. [Currently amended] Method for managing connections within a communications system, comprising the steps of:

configuring an outer IP security connection;

communicating from a client to a gateway on said outer connection a request to configure a secure inner connection;

responsive to said request, initializing said gateway to receive a future nested communication, including obtaining a client address from a packet on said outer connection;

starting said inner connection;

responsive to starting said inner connection, propagating a network address translation rule from said outer connection to said inner connection.

4. [Original] The method of claim 3, further comprising the step of:

further responsive to starting said inner connection, encapsulating a packet outbound from said gateway first in said inner connection and then in said outer connection.

5. [Original] The method of claim 4, further comprising the steps of:

responsive to receiving a packet at said gateway, determining if said packet has a security header;

responsive to said packet having said security header, decapsulating said packet and saving any address translation rule included within said packet; and

applying said address translation rule to said packet and thereafter communicating said packet from said gateway to said client.

6. [Original] The method of claim 5, further comprising the steps of:

iteratively executing said decapsulating step until a resulting decapsulated packet no longer contains a security header.

7. [Currently amended] Method for enabling a local gateway to handle dynamically assigned IP addresses from remote clients, comprising the steps of:

assigning said IP address to a remote client;

automatically maintaining between said remote client and said gateway nested IP security connections with local coincident endpoints.

8. [Original] The method of claim 7, wherein said nested connections comprise an inner connection and an outer connection.

9. [Currently amended] The method of claim 8, further comprising the steps of:

responsive to receiving ~~a nested~~ an inbound nested packet from said client on said outer connection, decapsulating said packet into a first packet and then performing source-in network address translation on said first packet; and

responsive to receiving ~~a second~~ an outbound second packet at said inner connection, performing source-in network address translation on said second packet, and then encapsulating said second packet into a nested packet for communication on said outer connection to client.

10. [Currently amended] System for operating a first node in a network including at least one second node, comprising:

an inner IP security connection;

an outer IP security connection;

a local coincident endpoint for said outer connection and said inner connection at said first node with respect to at least one second node;

said first node being responsive to receiving ~~a nested~~ an inbound nested packet from said second node on said outer connection for decapsulating said packet into a first packet and then performing source-in network address translation on said first packet; and

said first node being further responsive to receiving ~~a second~~ an outbound second packet at said inner connection for performing source-in network address translation on said second packet, and then encapsulating said second packet into a nested packet for communication on said outer connection to said second node.

11. [Currently amended] Method for extending virtual private network (VPN) network address translation (NAT) to include support for nested connections with coincident endpoints, without requiring any special configuration for the inner (nested) VPN connection, with respect to VPN NAT, comprising the steps of:

configuring an outer IP security connection with a VPN NAT rule;

communicating from a client to a gateway on said outer connection a dynamically generated security association request packet to configure a secure inner connection;

responsive to said request, initializing said gateway to receive a future nested communication, including obtaining a client address from said request packet on said outer connection;

starting said inner connection;

responsive to starting said inner connection, propagating said VPN NAT rule from said outer connection to said inner connection.

12. [Original] The method of claim 11, further comprising the step of:

further responsive to starting said inner connection, encapsulating a packet outbound from said gateway first in said inner connection and then in said outer connection.

13. [Original] The method of claim 12, further comprising the steps of:

responsive to receiving a packet at said gateway, determining if said packet has a security header;

responsive to said packet having said security header, decapsulating said packet and saving any VPN NAT rule included within said packet; and

applying said NAT rule to said packet and thereafter communicating said packet from said gateway to said client.

14. [Original] The method of claim 13, further comprising the step of:

iteratively executing said decapsulating step until a resulting decapsulated packet no longer contains a security header.

15. [Canceled]

16. [Currently amended] System for extending virtual private network (VPN) network address translation (NAT) to include support for nested connections with coincident endpoints, without requiring any special configuration for the inner (nested) VPN connection, with respect to VPN NAT, comprising:

a gateway;

a client;

an inner IP security connection for connecting said gateway and said client;

an outer IP security connection for connecting said gateway and said client;

said outer connection being configured by said client with a VPN NAT rule;

said outer connection for communicating from said client to said gateway a dynamically generated security association request packet to configure said inner connection;

said gateway further responsive to said request for initializing said gateway to receive a future nested communication, including obtaining a client address from said request packet on said outer connection;

said gateway further responsive to starting said inner connection for propagating said VPN NAT rule from said outer connection to said inner connection.

17. [Currently amended] A program storage device readable by a machine, tangibly embodying a program of instructions executable by a machine to perform method steps for operating a first node in a network including at least one second node, said method steps comprising:

establishing at said first node a coincident endpoint for an outer connection and an inner connection with respect to at least one second node, said outer connection and said inner connection being IP security connections;

responsive to receiving ~~a nested~~ an inbound nested packet from said second node on said outer connection, decapsulating said packet into a first packet and then

performing source-in network address translation on said first packet; and

responsive to receiving ~~a second~~ an outbound second packet at said inner connection, performing source-in network address translation on said second packet, and then encapsulating said second packet into a nested packet for communication on said outer connection to said second node.

18. [Currently amended] A computer program product or computer program element for operating a first node in a network including at least one second node according to the steps of:

establishing at said first node a coincident endpoint for an outer connection and an inner connection with respect to at least one second node, said outer connection and said inner connection being IP security connections;

responsive to receiving ~~a nested~~ an inbound nested packet from said second node on said outer connection, decapsulating said packet into a first packet and then

performing source-in network address translation on said first packet; and

responsive to receiving ~~a second~~ an outbound second packet at said inner connection, performing source-in network address translation on said second packet, and then encapsulating said second packet into a nested packet for communication on said outer connection to said second node.

19. [Currently amended] A program storage device readable by a machine, tangibly embodying a program of instructions executable by a machine to perform method steps for managing connections within a communications system, said method steps comprising:

configuring an outer IP security connection;

communicating from a client to a gateway on said outer connection a request to configure a secure inner connection;

responsive to said request, initializing said gateway to receive a future nested communication, including

obtaining a client address from a packet on said outer connection;

starting said inner connection;

responsive to starting said inner connection, propagating a network address translation rule from said outer connection to said inner connection.

20. [Original] The storage device of claim 19, said method steps further comprising the step of:

further responsive to starting said inner connection, encapsulating a packet outbound from said gateway first in said inner connection and then in said outer connection.

21. [Original] The storage device of claim 20, said method steps further comprising the steps of:

responsive to receiving a packet at said gateway, determining if said packet has a security header;

responsive to said packet having said security header,

decapsulating said packet and saving any address translation rule included within said packet; and

applying said address translation rule to said packet and thereafter communicating said packet from said gateway to said client.

22. [Original] The storage device of 21, said method steps further comprising the steps of:

iteratively executing said decapsulating step until a resulting decapsulated packet no longer contains a security header.